#3

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 실용신안등록출원 2000년 제 15161 호
Application Number

출 원 년 월 일 : 2000년 05월 29일
Date of Application

출 원 인 : 주식회사 퓨쳐시스템
Applicant(s)

CERTIFIED COPY OF PRIORITY DOCUMENT

2001 년 03 월 20 일

특 허 청
COMMISSIONER

【서류명】 실용신안등록출원서
【수신처】 특허청장
【제출일자】 2000.05.29
【고안의 명칭】 네트워크 모니터링을 위한 네트워크 시스템
【고안의 영문명칭】 Network system with networking monitoring function
【출원인】
【명칭】 주식회사 퓨쳐시스템
【출원인코드】 1-1998-004100-4
【대리인】
【성명】 이정익
【대리인코드】 9-1998-000410-4
【포괄위임등록번호】 2000-006349-7
【고안자】
【성명의 국문표기】 김광태
【성명의 영문표기】 KIM,Kwang tae
【주민등록번호】 591203-1540629
【우편번호】 463-030
【주소】 경기도 성남시 분당구 분당동 113 건영빌라 302동 106호
【국적】 KR
【기술평가청구사항】
【기술평가청구의 취지】 " 실용신안등록출원은 그 실용신안등록을 유지한다."라 는 결정을 구함
【청구항수】 5
【청구항】 1,2,3,4,5
【등록증 수령방법】 직접 (서울송달함)
【취지】 실용신안법 제9조의 규정에 의한 출원, 실용신안법 제21조 제1항의 규정에 의한 실용신안기술평가를 청구합니다. 대리인 이정익 (인)
【수수료】

【기본출원료】	18 면	20,000 원
【가산출원료】	0 면	0 원
【최초1년분등록료】	5 항	41,000 원
【우선권주장료】	0 건	0 원
【기술평가청구료】	5 항	156,000 원

【합계】	217,000 원
【감면사유】	중소기업
【감면후 수수료】	186,500 원
【첨부서류】	1. 요약서·명세서(도면)_1통 2.중소기업법시행령 제2조에의한 중소기업에 해당함을 증명하는 서류 _1통

【요약서】

【요약】

본 고안은 네트워크 모니터링을 위한 네트워크 시스템에 관한 것으로, 이 네트워크 시스템은 적어도 하나 이상의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와; 상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와; 상기 내부 네트워크와 상기 외부 네트워크를 연결하는 라우터와; 상기 외부 네트워크를 통한 외부 침입으로부터 상기 내부 네트워크의 내부 자원을 보호하기 위한 침입 차단 수단을 구비하고 있고, 특히 상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지할 수 있도록, 또한 상기 내부 네트워크 및 상기 외부 네트워크를 통한 내, 외부 공격에 의해 탐지되지 않도록, 상기 침입 차단 수단에 병렬 연결된 네트워크 모니터링 수단을 더 구비하고 있다.

【대표도】

도 4

【색인어】

내부 네트워크, 라우터, 외부 침입, 침입 차단, 네트워크 모니터링

【명세서】

【고안의 명칭】

네트워크 모니터링을 위한 네트워크 시스템{Network system with networking monitoring function}

【도면의 간단한 설명】

도 1은 종래의 네트워크 시스템의 구성도.

도 2는 종래의 네트워크 모니터링을 위한 네트워크 시스템의 구성도.

도 3은 종래의 다른 네트워크 모니터링을 위한 네트워크 시스템의 구성도.

도 4는 본 고안의 일실시예에 따른 네트워크 모니터링을 위한 네트워크 시스템의 구성도.

도 5는 본 고안이 적용된 사설 네트워크 시스템의 구성도.

* 도면의 주요 부분에 대한 부호의 설명

400 : 내부 네트워크 430 : 보안 게이트웨이

440 : 라우터 450 : 외부 네트워크

560 : 네트워크 모니터링 수단

【고안의 상세한 설명】

【고안의 목적】

【고안이 속하는 기술분야 및 그 분야의 종래기술】

<10> 본 고안은 네트워크 모니터링을 위한 네트워크 시스템에 관한 것으로, 특히 외부 침입으로부터 가상 사설 네트워크(VPN : Virtual Private Network)의 내부 자원을 보호하기 위한 네트워크 시스템에 관한 것이다.

<11> 일반적으로, 외부 네트워크, 예컨대 인터넷의 사용자들로부터 가상 사설 네트워크와 같은 내부 네트워크의 자원을 보호하는 역할을 수행하는 방화벽(firewall)은 인터넷의 사용자들이 내부 네트워크의 공개되지 않은 내부 자원에 접근하는 것을 막고, 자기 회사(내부 네트워크에 대응)의 직원들이 접속해야 할 외부의 자원들을 통제하기 위해 기업의 내부 네트워크와 인터넷 사이에 설치된다.

<12> 이와 같은 방화벽은 라우터(router)와 밀접하게 동작하며, 인터넷으로부터의 모든 입력 패킷을 내부 네트워크의 내부로 전달할 것인 지의 여부를 결정하기 위해 상기 입력 패킷을 검사하는 작업을 수행한다.

<13> 방화벽은 네트워크의 다른 부분들과는 별개로, 특별히 지정된 컴퓨터에 설치되는 경우가 많은데, 이는 인터넷과 같은 외부 네트워크로부터의 입력 패킷이 내부 네트워크의 내부 자원으로 곧바로 전달되지 않도록 하기 위한 것이다.

<14> 방화벽의 차폐 방법에는 몇 가지가 있다. 단순한 방법 중 한가지는 인터넷과 같은 외부 네트워크로부터 입력되는 요구, 즉 입력 패킷이 받아들일만한(즉, 이전에 확인된) 도메인 이름이나 IP 주소로부터 발생된 것인지를 확인하는 것이다. 이동 중인 사용자들

을 위해서는 보안 접속 절차나 인증 확인 등을 통해 사설 네트워크에 원격 접속할 수 있도록 허용한다.

<15> 침입 탐지 시스템으로서 방화벽 제품들을 만드는 회사들은 꽤 있다. 방화벽에 포함되어야할 기능으로는, 사용 기록, 보고, 공격이 시작된 시점에서의 자동 경보, 그리고 방화벽의 제어를 위한 그래픽 사용자 인터페이스 등이 있다.

<16> 위에서 언급한 가상 사설 네트워크(VPN)는 터널링 프로토콜과 보안 절차 등을 사용하여 공중 통신 네트워크 기반 시설을 개별 기업의 목적에 맞게 구성한 데이터 네트워크이다. 이와 같은 가상 사설 네트워크는 오직 한 회사에 의해서만 사용될 수 있는 자체 네트워크나 전용 회선과 대비되는 개념이다. 가상 사설 네트워크는 모든 회사들이 개별적으로 회선을 임차하는 것보다는 공중망을 공유함으로써 비용은 낮추면서도 전용 회선과 거의 동등한 서비스를 제공하려는 아이디어에서 출발하였다. 전화 회사들은 음성 메시지에 대해 보안이 유지되는 공유 자원을 제공한다. 가상 사설 네트워크는 데이터를 위해서도 역시 보안이 유지되는 공중망 자원의 공유를 가능하도록 한다. 오늘날 가상 사설 네트워크를 원하는 회사들은 주로 엑스트라넷이나 넓은 지역에 퍼져있는 지사들 간의 인트라넷에 이를 이용한다.

<17> 가상 사설 네트워크는 공중망을 통해 데이터를 송신하기 전에 데이터를 암호화하며, 수신측에서는 암호화된 데이터에 대해 복호화를 수행한다 (암호를 다시 푼다). 암호화는 데이터뿐 아니라, 부가적인 차원의 보안으로서 송수신지의 네트워크 주소도 포함된다. 마이크로소프트, 3Com 그리고 몇몇 다른 회사들이 PPTP (Point-to-Point Tunneling Protocol)라는 표준 프로토콜을 제안하였으며, 마이크로소프트는 이 프로토콜을 윈도우 NT 서버에 내장시켰다. 마이크로소프트의 PPTP

와 같은 VPN 소프트웨어는 대개 회사의 방화벽 서버에 설치되는 보안 소프트웨어도 마찬가지로 지원한다.

<18> 이와 같은 가상 사설 네트워크와 같은 내부 네트워크와 인터넷과 같은 외부 네트워크는 라우터에 의해 연결된다. 라우터는 동일한 전송 프로토콜을 사용하는 분리된 네트워크, 즉 상기 내부 네트워크와 상기 외부 네트워크를 연결하는 장치로 네트워크 계층간 서로 연결한다. 라우터는 여러 경로 중 가장 효율적인 경로를 선택하여 네트워크 패킷을 전송하고, 또한 흐름 제어를 수행하며, 내부 네트워크 내부에서 여러 서브 네트워크를 구성하고, 다양한 네트워크 관리 기능을 수행한다.

<19> 도 1에는 종래의 네트워크 시스템이 개략적으로 도시되어 있다. 이 종래의 네트워크 시스템은, 도 1에 도시된 바와 같이, 적어도 하나 이상의 서버(110)와 복수의 클라이언트(간략히 하기 위해 2 개의 클라이언트만이 도시되어 있음)(120a, 120b)로 구성된 내부 네트워크(100)를 구비하고 있다. 이 내부 네트워크(100)는 위에서 언급한 가상 사설 네트워크일 수 있다.

<20> 종래의 네트워크 시스템은 또한 외부 네트워크(150)를 포함하고 있으며, 이 외부 네트워크(150)로는 역시 위에서 언급한 바와 같이 인터넷을 들 수 있다.

<21> 종래의 네트워크 시스템은 또한 상기 내부 네트워크(100)와 상기 외부 네트워크(150)를 연결하기 위한 라우터(140)를 포함하고 있다. 라우터(140)는 위에서 언급한 바와 같이, 동일한 전송 프로토콜을 사용하는 분리된 네트워크, 즉 상기 내부 네트워크(100)와 상기 외부 네트워크(150)를 연결하기 위한 장치이다.

<22> 종래의 네트워크 시스템은 또한 상기 내부 네트워크(100)와 상기

라우터(140) 사이에 설치되어 있는 방화벽(130)을 구비하고 있다. 방화벽(130)은 외부 네트워크(150)의 사용자들로부터 내부 네트워크(100)의 내부 자원을 보호하기 위하여, 외부 네트워크(150)의 사용자들이 상기 내부 네트워크(100)의 공개되지 않은 자원에 접근하는 것을 막는 역할을 한다. 상기 방화벽은 유사한 기능의 장치에 의해서 대체될 수 있다. 예컨대, 상기 방화벽 대신에 보안 게이트웨이를 사용할 수도 있다.

<23> 도 2에는 종래의 네트워크 모니터링을 위한 네트워크 시스템이 도시되어 있다. 도 2의 종래의 네트워크 모니터링을 위한 네트워크 시스템은 내부 네트워크(200)와 방화벽(230) 사이에 네트워크 모니터링 시스템(260)이 설치되어 있다는 점을 제외하고는 도 1의 구성과 실질적으로 동일하다. 따라서, 동일한 부분에 대해서는 상세히 설명하지 않는다.

<24> 상기 네트워크 모니터링 시스템(260)은 앞단의 방화벽(230)을 통과한 입력 패킷에 대해서만 침입 여부를 탐지할 수 있다. 즉, 도 2에 표시된 바와 같이, 네트워크 모니터링 시스템(260)의 침입 탐지 범위는 'a'에 불과하다. 따라서, 방화벽(230)에 대한 직접적인 외부 공격과, 방화벽(230)의 앞단에 대한 외부 공격은 탐지할 수 없게 된다. 이로 인해, 상기 종래 시스템에 의해서는 완전한 보안 정책을 수립할 수 없고, 방화벽 자체에 대한 외부 공격으로 인해 방화벽이 외부 공격자에게 점유될 경우에는 내부 네트워크가 공격자에게 무방비 상태로 될 수 있다.

<25> 도 3에는 종래의 다른 네트워크 모니터링을 위한 네트워크 시스템이 도시되어 있다. 이 네트워크 시스템은 방화벽(330)과 라우터(340) 사이에 네트워크 모니터링 시스템(360)이 설치되어 있는 점을 제외하고는 도 1의 구성과 실질적으로 동일하다. 따라서, 도 1의 구성과 동일한 부분에 대해서는 상세히 설명하지 않는다. 도 3에서, 상기

네트워크 모니터링 시스템(360)은 방화벽(330)의 앞단의 침입 여부는 탐지할 수 있다. 즉, 도 3에 표시된 바와 같이, 네트워크 모니터링 시스템(360)의 침입 탐지 범위는 방화벽(330)의 앞단에서부터 내부 네트워크(300)까지, 즉 'b'이다.

<26> 이와 같이 방화벽(330)의 앞단에 네트워크 모니터링 시스템(360)을 설치한 경우에는, 상기 네트워크 모니터링 시스템(360) 자체가 외부 네트워크(350)로부터의 외부 공격자의 직접적인 공격 대상이 될 수 있으며, 최악의 경우에는 네트워크 침입을 위한 공격자의 침입 발판이 될 수 있다.

【고안이 이루고자 하는 기술적 과제】

<27> 본 고안은 위에서 언급한 종래의 문제점들을 해결하기 위한 것으로, 라우터에서부터 내부 네트워크까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지할 수 있도록; 또한 네트워크 모니터링 시스템이 외부 네트워크를 경유하게 되는 외부 공격자에 의해 탐지되지 않는 네트워크 시스템을 제공하는데 목적이 있다.

<28> 본 고안의 다른 목적은 라우터에서부터 내부 네트워크까지의 모든 네트워크 패킷에 대해 바이러스 검사를 할 수 있도록, 또한 안티 바이러스 시스템이 외부 네트워크를 경유하게 되는 외부 공격자에 의해 탐지되지 않는 네트워크 시스템을 제공하는데 있다.

【고안의 구성 및 작용】

<29> 상기 목적을 달성하기 위하여, 본 고안의 일측면에 따른 네트워크 모니터링을 위한 네트워크 시스템은 단일의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와; 상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와; 상기 내부 네트워크와 상

기 외부 네트워크를 연결하는 라우터와; 상기 외부 네트워크를 통한 외부 침입으로부터 상기 내부 네트워크의 내부 자원을 보호하기 위한 침입 차단 수단을 구비하고 있고, 특히 상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지할 수 있도록, 또한 상기 내부 네트워크 및 상기 외부 네트워크를 통한 내,외부 공격에 의해 탐지되지 않도록, 상기 침입 차단 수단에 병렬 연결된 네트워크 모니터링 수단을 더 구비하고 있다.

<30> 본 고안의 다른 측면에 따른 네트워크 시스템은 적어도 하나 이상의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와; 상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와; 상기 내부 네트워크와 상기 외부 네트워크를 연결하는 라우터와; 상기 외부 네트워크를 통한 외부 침입으로부터 상기 내부 네트워크의 내부 자원을 보호하기 위한 침입 차단 수단을 구비하고 있고, 특히 상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 바이러스 검사를 할 수 있도록, 또한 상기 내부 네트워크 및 상기 외부 네트워크를 통한 내,외부 공격에 의해 탐지되지 않도록, 상기 침입 차단 수단에 병렬 연결된 안티 바이러스 수단을 더 구비하고 있다.

<31> 본 고안의 또 다른 측면에 따른 네트워크 시스템은 적어도 하나 이상의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와; 상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와; 상기 내부 네트워크와 상기 외부 네트워크를 연결하는 라우터와; 상기 외부 네트워크를 통한 외부 침입으로부터 상기 내부 네트워크의 내부 자원을 보호하기 위한 침입 차단 수단을 구비하고 있고, 특히 상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지하고 바이러스 검사를 할 수 있도록, 또한 상기 내부 네트워크 및 상기 외부 네트워크를 통한 내,외부 공격에 의해

탐지되지 않도록, 상기 침입 차단 수단에 각각 병렬 연결된 네트워크 모니터링 수단 및 안티 바이러스 수단을 더 구비하고 있다.

<32> 상기 내부 네트워크는 가상 사설 네트워크(VPN) 등일 수 있고, 상기 침입 차단 시스템은 보안 게이트웨이 또는 방화벽 등일 수 있다.

<33> 이와 같이, 본 고안에 따라, 네트워크 모니터링 시스템을 방화벽이나 보안 게이트웨이에 병렬 연결하여 설치함으로써, 라우터에서부터 내부 네트워크까지의 모든 영역에 대해 네트워크 모니터링을 수행할 수 있고, 방화벽이나 보안 게이트웨이에 시도되는 공격을 탐지할 수 있어, 보다 완전을 보안을 달성할 수 있게 된다.

<34> 또한, 네트워크 모니터링 시스템 대신에 안티바이러스 시스템을 설치하면, 모든 패킷에 대해 바이러스 검사를 수행할 수 있고, 네트워크 모니터링 시스템과 안티 바이러스 시스템을 모두 설치함으로써 보다 완전한 보안 정책을 수립할 수도 있다.

<35> 이하에서는 첨부 도면을 참조하여 본 고안의 여러 가지 실시예에 대하여 설명한다.

<36> 도 4에는 본 고안의 일실시예에 따른 네트워크 모니터링을 위한 네트워크 시스템의 구성이 도시되어 있다. 도 4에 도시된 바와 같이, 본 고안에 따른 네트워크 모니터링을 위한 네트워크 시스템은, 단일의 서버(410)와 복수의 클라이언트(간략히 하기 위해 2 개의 클라이언트만이 도시되어 있음)(420a, 420b)로 구성된 내부 네트워크(400)를 구비하고 있다. 이 내부 네트워크(410)는 종래 기술을 설명하는 부분에서 언급한 가상 사설 네트워크일 수 있다.

<37> 본 고안의 네트워크 시스템은 또한 상기 내부 네트워크(400)로부터 분리되어 있는 외부 네트워크(450)를 포함하고 있으며, 이 외부 네트워크(450)로는 역시 위에서 언급한

바와 같이 인터넷을 들 수 있다.

<38> 본 고안의 네트워크 시스템은 또한 상기 내부 네트워크(400)와 상기 외부 네트워크(450)를 연결하기 위한 라우터(440)를 포함하고 있다. 이 라우터(440)는 동일한 전송 프로토콜을 사용하는 분리된 네트워크, 즉 상기 내부 네트워크(400)와 상기 외부 네트워크(450)를 연결하기 위한 장치이다.

<39> 본 고안의 네트워크 시스템은 또한 상기 내부 네트워크(400)와 상기 라우터(440) 사이에 보안 게이트웨이(430)를 구비한다. 이 보안 게이트웨이(430)는 외부 네트워크(450)의 사용자들로부터 내부 네트워크(400)의 내부 자원을 보호하기 위하여, 외부 네트워크(450)의 사용자들이 상기 내부 네트워크(400)의 공개되지 않은 자원에 접근하는 것을 막고, 자기 회사(내부 네트워크에 대응)의 직원들이 접속해야 할 외부의 자원들을 통제하도록 되어 있다. 상기 보안 게이트웨이(430)와 같은 보안장치는 유사한 기능의 장치에 의해 대체될 수 있다. 예컨대, 상기 보안 게이트웨이 대신에 방화벽을 사용할 수도 있다.

<40> 본 고안의 네트워크 시스템은 또한 네트워크 모니터링 시스템(460)을 구비하고 있으며, 이 네트워크 모니터링 시스템(460)은, 도 4에 도시된 바와 같이, 상기 라우터(440)에서부터 상기 내부 네트워크(400)까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지할 수 있도록, 또한 상기 외부 네트워크(450)를 통한 외부 공격에 의해 탐지되지 않도록, 상기 보안 게이트웨이(430)에 병렬 연결되어 있다.

<41> 이와 같이, 네트워크 모니터링 시스템(460)을 상기 보안 게이트웨이(430)에 병렬 설치함으로써, 본 고안에서는 네트워크 모니터링 시스템(460)의 침입 탐지 범위가 'a1 + a2

'로 된다. 즉, 상기 네트워크 모니터링 시스템(460)은 상기 라우터(440)에서부터 상기 내부 네트워크(400)까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지할 수 있다. 또한, 상기 네트워크 모니터링 시스템(460)은 보안 게이트웨이(430)에 병렬 설치되어 있기 때문에, 즉, 네트워크 내부나 외부에서 탐지되지 않는 블랙 존(black zone)에 위치하기 때문에, 상기 네트워크 모니터링 시스템(460)은 상기 내부 네트워크(400)의 사용자 및 상기 외부 네트워크(450)를 통해 공격을 하게 되는 외부 공격자에 의해 탐지되지 않게 된다. 따라서, 확실한 내부 감시를 행할 수 있고, 외부 공격자를 역추적할 수도 있다.

<42> 도 5에는, 본 고안의 다른 실시예에 따른 네트워크 시스템의 구성이 도시되어 있다. 이 네트워크 시스템은 사내 네트워크에 적용된 것으로 전체적인 구성은 도 4의 것과 동일하므로, 여기서는 상세 설명하지 않는다. 도 5에 도시된 바와 같이, 사내 네트워크 응용에서, 보안 게이트웨이(530)에 병렬로 네트워크 모니터링 시스템(560)이 설치되어 있음을 알 수 있다.

<43> 본 고안의 다른 실시예에 따라, 다른 기능을 가진 네트워크 모니터링 시스템을 사용하여 여러 가지 기능을 관리자에게 제공하여 여러 가지 응용에서 호환성을 유지할 수 있다. 예컨대, 본 고안의 네트워크 모니터링 시스템은 방화벽이나 보안 게이트웨이 등에 병렬로 연결 설치된 관계로, 내부 네트워크 내에서의 그 존재가 외부 공격자에 의해 탐지되지 않으므로, 상기 네트워크 모니터링 시스템은 외부 공격자를 역추적할 수도 있다.

<44> 본 고안의 또 다른 실시예에 따라, 상기와 같은 네트워크 모니터링 시스템 대신에 안티 바이러스 시스템을 마찬가지 방법으로 설치하면, 라우터에서부터 내부 네트워크까지의 모든 네트워크 패킷에 대해 바이러스 체크를 할 수 있다.

<45> 본 고안의 또 다른 실시예에 따라, 상기 네트워크 모니터링 시스템과 안티 바이러스 시스템을 함께 설치하면, 각각의 기능을 모두 활용할 수 있게 된다.

【고안의 효과】

<46> 이상에서와 같이, 본 고안에 따라 네트워크 모니터링 시스템을 방화벽, 보안 게이트웨이 또는 유사 기능의 장치에 병렬 연결하여 설치함으로써, 라우터에서부터 내부 네트워크까지의 모든 영역에 대해 네트워크 모니터링을 수행할 수 있고, 방화벽, 보안 게이트웨이 또는 유사 기능의 장치에 시도되는 공격을 탐지할 수 있어, 보다 완전한 보안을 달성할 수 있다.

<47> 본 고안의 네트워크 모니터링 시스템은 방화벽, 보안 게이트웨이 또는 유사 기능의 장치에 의해 필터링된 모든 네트워크 패킷을 확인, 탐지하여 통계 자료를 관리자에게 제공할 수 있으므로, 공격자의 공격 패턴을 알 수 있기 때문에, 그 공격 패턴을 연구하여 완전한 보안 정책을 수립할 수도 있다.

<48> 또한, 네트워크 모니터링 시스템의 모니터링 능력과 종류에 따라 호환성이 있는 다양한 기능과 서비스를 제공할 수도 있으며, 특히 네트워크 모니터링 시스템 대신에 안티 바이러스 시스템을 설치하면, 모든 패킷에 대해 바이러스 검사를 수행할 수 있고, 네트워크 모니터링 시스템과 안티바이러스 시스템을 모두 설치함으로써 보다 완전한 보안 정책을 수립할 수도 있다.

<49> 본 고안은 네트워크 모니터링 시스템이 자체 룰에 의해 네트워크 모니터링 시스템에 걸리는 부하를 줄일 수 있다.

<50> 본 고안은 여러 가지 바람직한 실시예를 참조하여 설명되었지만, 실용신안등록청구범위에 설명된 본 고안의 보다 넓은 취지 및 범위로부터 이탈하지 않고 상기 실시예에 대해 각종 수정이나 변형이 행해질 수 있음은 당업자에게 명백하다. 따라서, 명세서 및 도면은 제한적인 의미보다는 예시적인 것으로 간주되어야 한다.

【실용신안등록청구범위】

【청구항 1】

적어도 하나 이상의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와;

상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와;

상기 내부 네트워크와 상기 외부 네트워크를 연결하는 라우터와;

상기 외부 네트워크를 통한 외부 침입으로부터 상기 내부 네트워크의 내부 자원을 보호하기 위한 침입 차단 수단을 구비한 네트워크 모니터링을 위한 네트워크 시스템에 있어서,

상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지할 수 있도록, 또한 상기 내부 네트워크 및 상기 외부 네트워크를 통한 내, 외부 공격에 의해 탐지되지 않도록, 상기 침입 차단 수단에 병렬 연결된 네트워크 모니터링 수단을 더 구비한 것을 특징으로 하는 네트워크 모니터링을 위한 네트워크 시스템.

【청구항 2】

적어도 하나 이상의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와;

상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와;

상기 내부 네트워크와 상기 외부 네트워크를 연결하는 라우터와;

상기 외부 네트워크를 통한 외부 침입으로부터 상기 내부 네트워크의 내부 자원을 보호하기 위한 침입 차단 수단을 구비한 네트워크 모니터링을 위한 네트워크 시스템에 있어서,

상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 바이러

스 검사를 할 수 있도록, 또한 ㅊ 및 상기 외부 네트워크를 통한 내,외부 공격에 의해 탐지되지 않도록, 상기 침입 차단 수단에 병렬 연결된 안티 바이러스 수단을 더 구비한 것을 특징으로 하는 네트워크 모니터링을 위한 네트워크 시스템.

【청구항 3】

적어도 하나 이상의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와;

상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와;

상기 내부 네트워크와 상기 외부 네트워크를 연결하는 라우터와;

상기 외부 네트워크를 통한 외부 침입으로부터 상기 내부 네트워크의 내부 자원을 보호하기 위한 침입 차단 수단을 구비한 네트워크 모니터링을 위한 네트워크 시스템에 있어서,

상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 침입 여부를 탐지하고 바이러스 검사를 할 수 있도록, 또한 상기 내부 네트워크 및 상기 외부 네트워크를 통한 내,외부 공격에 의해 탐지되지 않도록, 상기 침입 차단 수단에 각각 병렬 연결된 네트워크 모니터링 수단과 안티 바이러스 수단을 더 구비한 것을 특징으로 하는 네트워크 모니터링을 위한 네트워크 시스템.

【청구항 4】

제 1 항 내지 제 3 항 중 어느 한 항에 있어서,

상기 내부 네트워크는 가상 사설 네트워크(VPN)인 것을 특징으로 하는 네트워크 모니터링을 위한 네트워크 시스템.

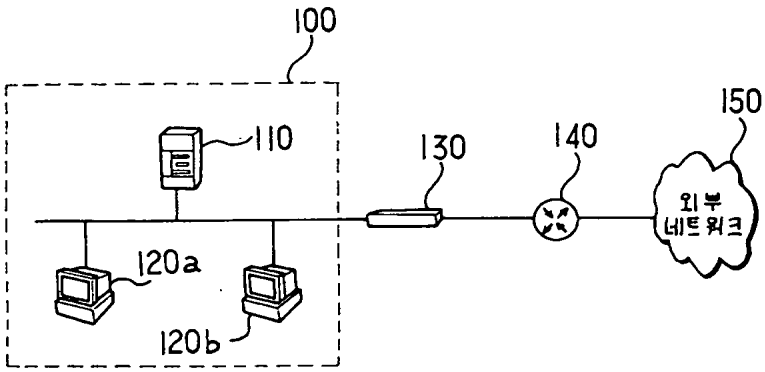
【청구항 5】

제 1 항 내지 제 3 항 중 어느 한 항에 있어서,

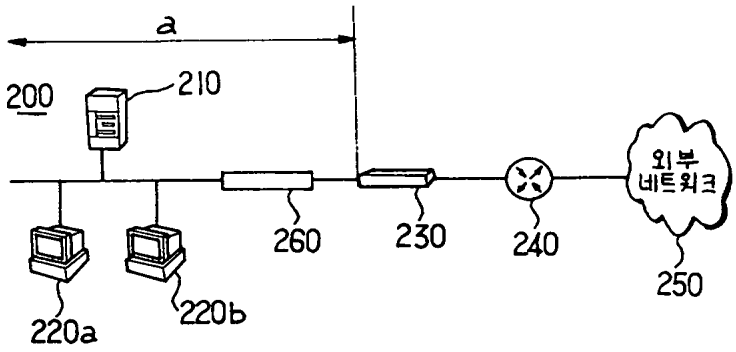
상기 침입 차단 수단은 보안 게이트웨이 또는 방화벽인 것을 특징으로 하는 네트워크 모니터링을 위한 네트워크 시스템.

【도면】

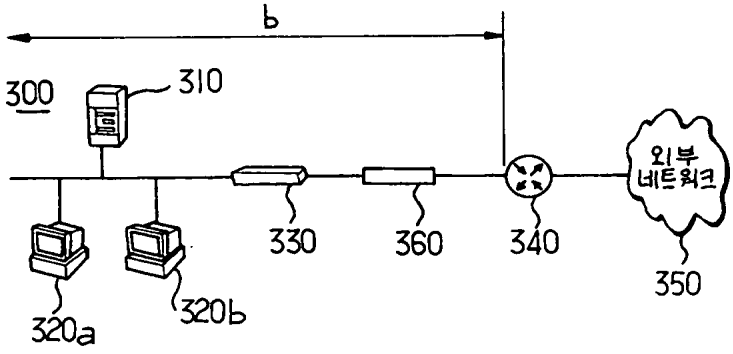
【도 1】


100
110
130
140
150
외부
네트워크
120a
120b

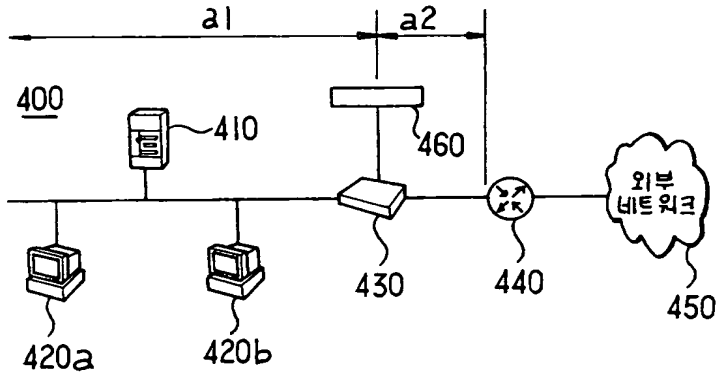
【도 2】


a
200
210
외부
네트워크
260
230
240
250
220a
220b

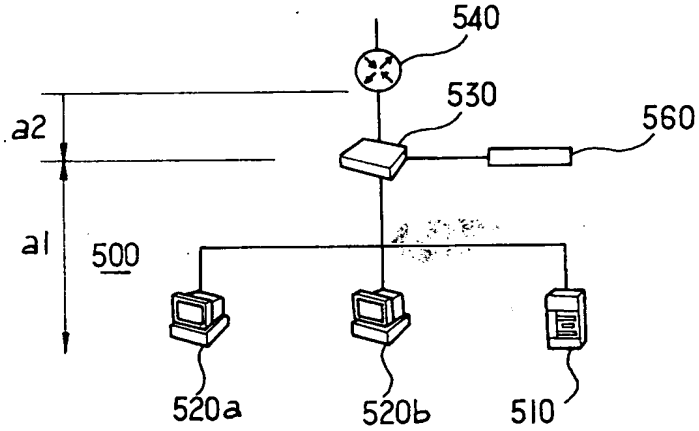
【도 3】


b
300
310
외부
네트워크
330
360
340
350
320a
320b

【도 4】


a1
a2
400
410
460
외부
네트워크
430
440
450
420a
420b

【도 5】


540
530
560
a2
a1
500
520a
520b
510

1020000015161 출력 일자: 2001/3/22

【서류명】 명세서 등 보정서
【수신처】 특허청장
【제출일자】 2000.06.12
【제출인】
【명칭】 주식회사 퓨쳐시스템
【출원인코드】 1-1998-004100-4
【사건과의 관계】 출원인
【대리인】
【성명】 이정익
【대리인코드】 9-1998-000410-4
【포괄위임등록번호】 2000-006349-7
【사건의 표시】
【출원번호】 20-2000-0015161
【출원일자】 2000.05.29
【고안의 명칭】 네트워크 모니터링을 위한 네트워크 시스템
【제출원인】
【접수번호】 1-1-00-0108633-72
【접수일자】 2000.05.29
【보정할 서류】 명세서등
【보정할 사항】
【보정대상 항목】 별지와 같음
【보정방법】 별지와 같음
【보정내용】 별지와 같음
【취지】 실용신안법시행규칙 제8조의 규정에 의하여 위와 같이 제출합니다. 대리인
이정익 (인)
【수수료】
【보정료】 0 원
【추가1년분등록료】 0 원
【기타 수수료】 0 원
【합계】 0 원
【첨부서류】 1. 기타첨부서류_1통[보정서 1통]

【보정대상항목】 청구항 2

【보정방법】 정정

【보정내용】

적어도 하나 이상의 서버와 복수의 클라이언트를 포함하고 있는 내부 네트워크와;

상기 내부 네트워크로부터 분리되어 있는 외부 네트워크와;

상기 내부 네트워크와 상기 외부 네트워크를 연결하는 라우터와;

상기 외부 네트워크를 통한 외부 침입으로부터 상기 내부 네트워크의 내부 자원을 보호하기 위한 침입 차단 수단을 구비한 네트워크 모니터링을 위한 네트워크 시스템에 있어서,

상기 라우터에서부터 상기 내부 네트워크까지의 모든 네트워크 패킷에 대해 바이러스 검사를 할 수 있도록, 또한 내부 네트워크 및 상기 외부 네트워크를 통한 내,외부 공격에 의해 탐지되지 않도록, 상기 침입 차단 수단에 병렬 연결된 안티 바이러스 수단을 더 구비한 것을 특징으로 하는 네트워크 모니터링을 위한 네트워크 시스템.